HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 10012790-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Philip M. WALKER et al.

Confirmation No.: 9299

Application No.: 09/903,278

Examiner: Tran, Tongoc

Filing Date: July 11, 2001

Group Art Unit: 2134

Title: SYSTEM AND METHOD OF VERIFYING SYSTEM ATTRIBUTES

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on June 1, 2007.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

☒ A duplicate copy of this transmittal letter is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: July 31, 2007

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.
Date of facsimile:
Typed Name: Cindy C. Dioso
Signature: Cindy C. Dioso

Respectfully submitted,

Philip M. WALKER et al.

By: James L Baudino

James L. Baudino

Attorney/Agent for Applicant(s)

Reg No.: 43,486

Date: July 31, 2007

Telephone: 214-855-7544

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	Philip M. WALKER et al.	Confirmation No.: 9299
Serial No.:	09/903,278	
Filing Date:	July 11, 2001	
Group Art Unit:	2134	
Examiner:	Tran, Tongoc	
Title:	SYSTEM AND METHOD OF VERIFYING SYSTEM ATTRIBUTES	
Docket No.:	10012790-1	

MAIL STOP: APPEAL BRIEF PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

APPEAL BRIEF

Appellants have appealed to the Board of Patent Appeals and Interferences from the decision of the Examiner mailed March 1, 2007, finally rejecting Claims 1-26. Appellants filed a Notice of Appeal on June 1, 2007. Appellants respectfully submit herewith this Appeal Brief with authorization to charge the statutory fee of $500.00.

REAL PARTY IN INTEREST

The present application was assigned to Hewlett-Packard Company as indicated by an assignment from the inventor recorded on January 9, 2002 in the Assignment Records of the United States Patent and Trademark Office at Reel 012462, Frame 0298. The present application was subsequently assigned to Hewlett-Packard Development Company, L.P. as indicated by an assignment from Hewlett-Packard Company recorded on September 30, 2003 in the Assignment Records of the United States Patent and Trademark Office at Reel 014061, Frame 0492. The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no known appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this pending appeal.

STATUS OF CLAIMS

Claims 1-26 stand rejected pursuant to a final Office Action mailed March 1, 2007 (hereinafter, the "Office Action"). Claims 1-26 are presented for appeal.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the mailing of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the present invention as defined by independent Claim 1 are directed toward a system comprising a target (16), a probe (18, 20) operable to execute in the target (16) and collect a predetermined set of data associated with the target (16), and a monitor (14) operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target (16) has been altered (at least at page 3, line 15 to page 4, line 17 and page 5, line 10 to page 6, line 21).

Embodiments of the present invention as defined by Claim 6 are directed toward the invention as defined by Claim 1, wherein the probe (18, 20) is operable to calculate a signature value of at least a portion of an execution image of the probe (18, 20) (at least at page 3, lines 24-25; page 5, lines 15-31; and page 6, lines 1-21).

Embodiments of the present invention as defined by Claim 8 are directed toward the invention as defined by Claim 1, wherein the probe (18, 20) is operable to determine a signature value of a random subset of an execution image of the probe (18, 20) (at least at page 3, lines 24-25; page 5, lines 15-31; and page 6, lines 1-21).

Embodiments of the present invention as defined by independent Claim 10 are directed toward a method comprising executing a probe (18, 20) in a target (16) and collecting a predetermined set of data associated with the target (16) for comparison with expected data values for the predetermined set of data to determine whether the target (16) has been altered (at least at page 3, line 15 to page 4, line 17 and page 5, line 10 to page 6, line 21).

Embodiments of the present invention as defined by Claim 15 are directed toward the invention as defined by Claim 10, further comprising calculating a signature value of at least a portion of the probe (18, 20) for comparison to an expected signature value (at least at page 3, lines 24-25; page 5, lines 15-31; and page 6, lines 1-21).

Embodiments of the present invention as defined by Claim 16 are directed toward the invention as defined by Claim 10, further comprising calculating a signature value of the probe (18, 20) for comparison to an expected signature value (at least at page 3, lines 24-25; page 5, lines 15-31; and page 6, lines 1-21).

Embodiments of the present invention as defined by independent Claim 19 are directed toward a method comprising initiating the execution of a probe (18, 20) in a target (16), receiving from the probe (18, 20) a predetermined set of data associated with the target (16), and comparing the received predetermined set of data with expected data values thereof to determine whether the target (16) has been altered (at least at page 3, line 15 to page 4, line 17 and page 5, line 10 to page 6, line 21).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-17, 19-24 and 26 are rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,978,475 issued to Schneier et al. (hereinafter "*Schneier*").

2. Claims 1, 10 and 19 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,088,804 issued to Hill et al. (hereinafter "*Hill*").

3. Claims 18 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Schneier*.

ARGUMENT

A. Standard

1. 35 U.S.C. § 102

Under 35 U.S.C. § 102, a claim is anticipated only if each and every element as set forth in the claim is found in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 2 U.S.P.Q.2d 1051 (Fed. Cir. 1987); M.P.E.P. § 2131. In addition, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claims" and "[t]he elements must be arranged as required by the claim." *Richardson v. Suzuki Motor Co.*, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989); *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990); M.P.E.P. § 2131.

2. 35 U.S.C. § 103

To establish a *prima facie* case of obviousness under 35 U.S.C. § 103, three basic criteria must be met: First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; second, there must be a reasonable expectation of success; and finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *In re Vaeck*, 947 F.2d 488, (Fed. Cir. 1991); M.P.E.P. § 2143. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *Id.* Further, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680 (Fed. Cir. 1990); M.P.E.P. § 2143.01. Additionally, not only must there be a suggestion to combine the functional or operational aspects of the

combined references, but also the prior art is required to suggest both the combination of elements and the structure resulting from the combination. *Stiftung v. Renishaw PLC*, 945 F.2d 1173, 1183 (Fed. Cir. 1991). Moreover, where there is no apparent disadvantage present in a particular prior art reference, then generally there can be no motivation to combine the teaching of another reference with the particular prior art reference. *Winner Int'l Royalty Corp. v. Wang*, 202 F.3d 1340, 1349 (Fed. Cir. 2000).

B. Argument

1. Rejection under 35 U.S.C. §102(b) over *Schneier*

a. Claims 1-5, 7, 9-14, 17, 19-24 and 26

Claims 1-5, 7, 9-14, 17, 19-24 and 26 were rejected under 35 U.S.C. §102(b) as being anticipated by *Schneier*. Of the rejected claims, Claims 1, 10 and 19 are independent. Appellants respectfully submit that each of independent Claims 1, 10 and 19 are patentable over *Schneier* and, therefore, Claims 2-5, 7, 9, 11-14, 17, 18-24 an 26 that depend respectively therefrom are also allowable.

Independent Claim 1, for example, recites "a target," "a probe operable to execute in the target and collect a predetermined set of data associated with the target" and "a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered."

Schneier appears to disclose an untrusted computer 102 (which the Appellee appears to consider as the "target" recited by Claim 1) having an audit logging program 200 for generating a secure audit log 300 (*Schneier*, column 4, lines 13-61). The Appellee appears to consider the audit logging program 200 of *Schneier* as corresponding to the "probe" recited by Claim 1 (Office action, pages 3 and 4). *Schneier* appears to disclose a cryptographic module 220 that is used in combination with the audit logging program 200 to protect the audit log 300 (*Schneier*, column 6, lines 12-21). *Schneier* also appears to disclose a trusted computer 101 and/or a verifier computer 103 that may be used to verify the audit log 300 (*Schneier*, column 13, lines 4-25). Thus, *Schneier* appears to be directed toward determining whether the audit log 300 has been tampered with or altered, and not whether the "target" or, in *Schneier*, the untrusted computer, has been altered. Thus, based on the foregoing, the *Schneier* reference appears to be directed toward determining whether the "predetermined set of data" (the audit log 300) is altered, instead of whether the untrusted computer 102 of *Schneier* (the "target") has been

altered. Accordingly, for at least this reason, Appellants respectfully submit that *Schneier* does not anticipate Claim 1.

Further, Claim 1 recites "a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered" (emphasis added). In the Office Action, the Appellee appears to consider the audit log 300 of *Schneier* as corresponding to the "predetermined set of data" recited by Claim 1 (Office Action, pages 3 and 4). *Schneier* appears to disclose that the audit log 300 of *Schneier* is a collection of entries indicating, for example, a type of action that is being logged, the person or computer that initiated the action, the results or effects of the action, successful and unsuccessful log-ins, log-offs, remote log-ins, etc. (*Schneier*, column 6, lines 42-64). Thus, the audit log 300 of *Schneier* appears to be data representative of entirely unexpected or random occurrences associated with a computer in *Schneier*. Thus, Appellants respectfully submit that the audit log 300 of *Schneier* is not "compare[d] with expected values" as recited by Claim 1 (emphasis added) to determine whether the target computer in *Schneier* has been altered ay least because the information of the audit log 300 of *Schneier* appears to be completely unexpected and/or random based on what acts or events happen to take place or occur with the computer of *Schneier*. Therefore, for at least this reason also, Appellants respectfully submit that Claim 1 is not anticipated by *Schneier*.

Independent Claim 10 recites "executing a probe in a target" and "collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered" (emphasis added). Independent Claim 19 recites "initiating the execution of a probe in a target," "receiving from the probe a predetermined set of data associated with the target" and "comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered" (emphasis added). At least for the reasons discussed above in connection with independent Claim 1, Appellants respectfully submit that independent Claims 10 and 19 are also not anticipated by *Schneier*.

Claims 2-5, 7, 9, 11-14, 17, 18-24 and 26 depend respectively from independent Claims 1, 10 and 19. Therefore, for at least this reason, Appellants respectfully submit that Claims 2-5, 7, 9, 11-14, 17, 18-24 an 26 are also allowable over *Schneier*.

Accordingly, for at least the reasons discussed above, independent Claims 1, 10 and 19 are clearly patentable over *Schneier*. Therefore, Claims 1, 10 and 19, and Claims 2-5, 7, 9, 11-14, 17, 18-24 and 26 that depend respectively therefrom, are in condition for allowance.

b. Claim 6

Claim 6 recites "wherein the probe is operable to calculate a signature value of at least a portion of an execution image of the probe" (emphasis added). In the Office Action, the Appellee asserts that column 8, line 45 to column 9, line 2, of *Schneier* discloses the limitations of Claim 6 (Office Action, page 5). Appellants disagree. *Schneier* appears to disclose a cryptographic module 220 that is used to protect the audit log 300 *Schneier* (*Schneier*, column 6, lines 12-21). *Schneier* also appears to disclose that various types of encryption/decryption techniques may be used to protect the audit log 300 data (*Schneier*, column 8, line 45 to column 9, line 2). However, *Schneier* does not appear to disclose or even suggest, in the portion of *Schneier* referred to by the Appellee or elsewhere in *Schneier*, that a signature value is calculated of "at least a portion of an execution image" of the audit logging program 200 of *Schneier* (which the Appellee considers to correspond to the "probe" recited by Claim 6 (Office Action, pages 2-4)). Therefore, for at least this reason, Appellants respectfully submit that Claim 6 is clearly patentable over *Schneier*.

c. Claim 8

Claim 8 recites "wherein the probe is operable to determine a signature value of a random subset of an execution image of the probe" (emphasis added). In the Office Action, the Appellee asserts that column 18, lines 23-28, of *Schneier* discloses the limitations of Claim 8 (Office Action, page 5). Appellants disagree. *Schneier* appears to disclose a cryptographic module 220 that is used to protect the audit log 300 *Schneier* (*Schneier*, column 6, lines 12-21). *Schneier* also appears to disclose that various types of encryption/decryption techniques may be used to protect the audit log 300 data (*Schneier*, column 8, line 45 to column 9, line 2, column 18, lines 23-28). However, *Schneier* does not appear to disclose or even suggest, in the portion of *Schneier* referred to by the Appellee or elsewhere in *Schneier*, that a signature value "of a random subset of an execution image" of the audit logging program 200 of *Schneier* (which the Appellee considers to correspond to the "probe" recited by Claim 8 (Office Action, pages 2-4)). Therefore, for at least this reason, Appellants respectfully submit that Claim 8 is clearly patentable over *Schneier*.

d. Claim 15

Claim 15 recites " calculating a signature value of at least a portion of the probe for comparison to an expected signature value" (emphasis added). In the Office Action, the Appellee asserts that column 8, line 45 to column 9, line 2, of *Schneier* discloses the limitations of Claim 15 (Office Action, page 5). Appellants disagree. *Schneier* appears to disclose a cryptographic module 220 that is used to protect the audit log 300 *Schneier* (*Schneier*, column 6, lines 12-21). *Schneier* also appears to disclose that various types of encryption/decryption techniques may be used to protect the audit log 300 data (*Schneier*, column 8, line 45 to column 9, line 2). However, *Schneier* does not appear to disclose or even suggest, in the portion of *Schneier* referred to by the Appellee or elsewhere in *Schneier*, that a signature value is calculated of "at least a portion of" the audit logging program 200 of *Schneier* (which the Appellee considers to correspond to the "probe" recited by Claim 15 (Office Action, pages 2-4)). Therefore, for at least this reason, Appellants respectfully submit that Claim 15 is clearly patentable over *Schneier*.

e. Claim 16

Claim 16 recites "calculating a signature value of the probe for comparison to an expected signature value" (emphasis added). In the Office Action, the Appellee asserts that column 8, line 45 to column 9, line 2, of *Schneier* discloses the limitations of Claim 16 (Office Action, page 5). Appellants disagree. *Schneier* appears to disclose a cryptographic module 220 that is used to protect the audit log 300 *Schneier* (*Schneier*, column 6, lines 12-21). *Schneier* also appears to disclose that various types of encryption/decryption techniques may be used to protect the audit log 300 data (*Schneier*, column 8, line 45 to column 9, line 2). However, *Schneier* does not appear to disclose or even suggest, in the portion of *Schneier* referred to by the Appellee or elsewhere in *Schneier*, that a signature value is calculated of the audit logging program 200 of *Schneier* (which the Appellee considers to correspond to the "probe" recited by Claim 16 (Office Action, pages 2-4)). Therefore, for at least this reason, Appellants respectfully submit that Claim 16 is clearly patentable over *Schneier*.

2. Rejection under 35 U.S.C. §102(b) over *Hill*

a. Claim 1

Claim 1 was rejected under 35 U.S.C. §102(e) as being anticipated by *Hill*. Appellants respectfully submit that independent Claim is patentable over *Hill*.

Hill appears to disclose a security agent 36 (which the Appellee appears to consider to correspond to the "probe" recited by Claim 1 (Office Action, page 6)) that detects occurrences of security events on a computer node (e.g., port scans, malicious software being operated on the node, and penetration attempts) (*Hill*, abstract, column 4, lines 30-41, column 10, lines 24-36). *Hill* also appears to disclose a SOM processor 40 that the Appellee appears to consider to correspond to the "monitor" recited by Claim 1 (Office Action, pages 3 and 6). *Hill* appears to disclose that the SOM processor 40 receives the security events from the security agent 36 of *Hill* and compares the events to training signatures to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). In the Office Action, the Appellee states that *Hill* teaches "comparing the received signature with the training signature" and thus encompasses "reading, comparing and determining the differences in the set of received data with another set of predetermined data" (Office Action, page 3). Appellants submit that the purported teaching of *Hill* does not anticipate Claim 1.

For example, the Appellee relies on the SOM processor 40 of *Hill* to "receive the collected predetermined set of data to compare with expected data values" as recited by Claim 1 (emphasis added). However, the Appellee appears to ignore the remainder of the above-referenced limitation of Claim 1, namely, that the monitor "receive[s] the collected predetermined set of data to compare with expected data values to determine whether the target has been altered" (emphasis added). In *Hill*, the SOM processor 40 of *Hill* appears to compare a signature received from the security agent 36 of *Hill* to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). *Hill* appears to disclose that the security events may include port scans, malicious software, penetration attempts, etc. (*Hill*, column 4, lines 31-41). Thus, the SOM processor 40 of *Hill* does not make any comparison "to determine whether the target has been altered" as recited by Claim 1. To the contrary, the SOM processor 40 is merely determining what action or response to take to an identified attack. Thus, Appellants submit that the SOM processor 40 of *Hill* is not making any comparison "to determine whether the target has been altered" as recited by Claim 1. Thus, for at least this reason, Appellants submit that *Hill* does not anticipate Claim 1.

b. Claim 10

Claim 10 was rejected under 35 U.S.C. §102(e) as being anticipated by *Hill*. Appellants respectfully submit that independent Claim 10 is patentable over *Hill*.

Independent Claim 10 recites "executing a probe in a target" and "collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered" (emphasis added). *Hill* appears to disclose a security agent 36 (which the Appellee appears to consider to correspond to the "probe" recited by Claim 10 (Office Action, page 6)) that detects occurrences of security events on a computer node (e.g., port scans, malicious software being operated on the node, and penetration attempts) (*Hill*, abstract, column 4, lines 30-41, column 10, lines 24-36). *Hill* also appears to disclose a SOM processor 40 that receives the security events from the security agent 36 of *Hill* and compares the events to training signatures to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). In the Office Action, the Appellee states that *Hill* teaches "comparing the received signature with the training signature" and thus encompasses "reading, comparing and determining the differences in the set of received data with another set of predetermined data" (Office Action, page 3). Appellants submit that the purported teaching of *Hill* does not anticipate Claim 10.

For example, in *Hill*, the SOM processor 40 of *Hill* appears to compare a signature received from the security agent 36 of *Hill* to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). *Hill* appears to disclose that the security events may include port scans, malicious software, penetration attempts, etc. (*Hill*, column 4, lines 31-41). Thus, the SOM processor 40 of *Hill* does not make any comparison "to determine whether the target has been altered" as recited by Claim 10. To the contrary, the SOM processor 40 is merely determining what action or response to take to an identified attack. Thus, Appellants submit that the SOM processor 40 of *Hill* is not making any comparison "to determine whether the target has been altered" as recited by Claim 10. Thus, for at least this reason, Appellants submit that *Hill* does not anticipate Claim 10.

c. Claim 19

Claims 19 was rejected under 35 U.S.C. §102(e) as being anticipated by *Hill*. Appellants respectfully submit that independent Claim 19 is patentable over *Hill*.

Independent Claim 19 recites "initiating the execution of a probe in a target," "receiving from the probe a predetermined set of data associated with the target" and "comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered" (emphasis added). *Hill* appears to disclose a security agent 36 (which

the Appellee appears to consider to correspond to the "probe" recited by Claim 19 (Office Action, page 6)) that detects occurrences of security events on a computer node (e.g., port scans, malicious software being operated on the node, and penetration attempts) (*Hill*, abstract, column 4, lines 30-41, column 10, lines 24-36). *Hill* also appears to disclose a SOM processor 40 that the Appellee appears to consider to receive the security events from the security agent 36 of *Hill* and compare with expected data values (Office Action, pages 3 and 6). *Hill* appears to disclose that the SOM processor 40 receives the security events from the security agent 36 of *Hill* and compares the events to training signatures to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). In the Office Action, the Appellee states that *Hill* teaches "comparing the received signature with the training signature" and thus encompasses "reading, comparing and determining the differences in the set of received data with another set of predetermined data" (Office Action, page 3). Appellants submit that the purported teaching of *Hill* does not anticipate Claim 19.

For example, the Appellee relies on the SOM processor 40 of *Hill* to "receiv[e] from the probe a predetermined set of data associated with the target" and "compare[] the received predetermined set of data with expected data values thereof to determine whether the target has been altered" as recited by Claim 19 (emphasis added). In *Hill*, the SOM processor 40 of *Hill* appears to compare a signature received from the security agent 36 of *Hill* to determine a recommended action or response to the attack (*Hill*, abstract, column 8, lines 35-53, column 10, lines 24-36). *Hill* appears to disclose that the security events may include port scans, malicious software, penetration attempts, etc. (*Hill*, column 4, lines 31-41). Thus, the SOM processor 40 of *Hill* does not make any comparison "to determine whether the target has been altered" as recited by Claim 19. To the contrary, the SOM processor 40 is merely determining what action or response to take to an identified attack. Thus, Appellants submit that the SOM processor 40 of *Hill* is not making any comparison "to determine whether the target has been altered" as recited by Claim 19. Thus, for at least this reason, Appellants submit that *Hill* does not anticipate Claim 19.

3. Rejection under 35 U.S.C. §103

a. Claims 18 and 25

Claims 18 and 25 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Schneier*. Claims 18 and 25 depend respectively from independent Claims 10 and 19. As indicated above, Claims 10 and 19 are patentable over *Schneier*. Therefore, for at least this reason, Claims 18 and 19 are also patentable over *Schneier*.

CONCLUSION

Appellants have demonstrated that the present invention as claimed is clearly distinguishable over the art cited of record. Therefore, Appellants respectfully request the Board of Patent Appeals and Interferences to reverse the final rejection of the Examiner and instruct the Examiner to issue a notice of allowance of all claims.

The Commissioner is authorized to charge the statutory fee of $500.00 to Deposit Account No. 08-2025 of Hewlett-Packard Company. Although no other fee is believed due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

James L. Baudino
Registration No. 43,486

Date: July 31, 2007

Correspondence To:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400
Tel. (970) 898-3884

CLAIMS APPENDIX

1. A system comprising:

a target;

a probe operable to execute in the target and collect a predetermined set of data associated with the target; and

a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered.

2. The system, as set forth in claim 1, wherein the probe is resident in the target.

3. The system, as set forth in claim 1, wherein the monitor is operable to send the probe to the target for execution.

4. The system, as set forth in claim 1, wherein the probe repeatedly executes and the predetermined set of data varies for each execution of the probe.

5. The system, as set forth in claim 1, wherein the predetermined set of data includes system attributes and system usage data.

6. The system, as set forth in claim 1, wherein the probe is operable to calculate a signature value of at least a portion of an execution image of the probe.

7. The system, as set forth in claim 1, wherein the monitor is operable to compare the calculated signature value to an expected signature value.

8. The system, as set forth in claim 1, wherein the probe is operable to determine a signature value of a random subset of an execution image of the probe.

9. The system, as set forth in claim 1, wherein the probe is operable to generate an encryption key from the signature value for encrypting the collected predetermined set of data.

10. A method comprising:

executing a probe in a target;

collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered.

11. The method, as set forth in claim 10, further comprising receiving a request to execute the probe resident in the target.

12. The method, as set forth in claim 10, further comprising receiving the probe and executing the received probe in the target.

13. The method, as set forth in claim 10, wherein the step of executing a probe is repeated.

14. The method, as set forth in claim 10, wherein the step of executing a probe comprises collecting a different predetermined set of data for each execution of the probe.

15. The method, as set forth in claim 10, further comprising calculating a signature value of at least a portion of the probe for comparison to an expected signature value.

16. The method, as set forth in claim 10, further comprising calculating a signature value of the probe for comparison to an expected signature value.

17. The method, as set forth in claim 16, further comprising:

generating an encryption key from the signature value; and

encrypting the collected predetermined set of data with the encryption key.

18. The method, as set forth in claim 17, further comprising:

sending the encrypted data to a monitor, the data including system attribute data and system usage data;

decrypting the encrypted data using a decryption key;

verifying the system attribute data; and

generating billing data based on the system usage data in response to the system attribute data being verified.

19. A method comprising:

initiating the execution of a probe in a target;

receiving from the probe a predetermined set of data associated with the target; and

comparing the received predetermined set of data with expected data values thereof to determine whether the target has been altered.

20. The method, as set forth in claim 19, further comprising sending a request to the probe resident in the target to initiate the execution.

21. The method, as set forth in claim 19, further comprising sending the probe and executing the probe in the target.

22. The method, as set forth in claim 19, wherein initiating the execution of a probe comprises repeating execution of the probe.

23. The method, as set forth in claim 19, wherein initiating the execution of a probe comprises collecting a different predetermined set of data for each execution of the probe.

24. The method, as set forth in claim 19, further comprising:

receiving collected data encrypted by the probe using an encryption key derived from a self-hash value, the data including system attribute data and system usage data;

decrypting the encrypted data; and

verifying the system attribute data.

25. The method, as set forth in claim 23, further comprising generating billing data based on the system usage data in response to the system attribute data being verified.

26. The method, as set forth in claim 19, further comprising:

receiving a reply containing at least the collected predetermined set of data, the data including system attribute data and system usage data; and

verifying the system attribute data.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None